Plaintiffs' Exhibit 66

Investigative Memorandum: App Technical Investigation

TO:	Gibson Dunn & Crutcher LLP
FROM:	Stroz Friedberg
DATE:	June 12, 2018
RE:	Social Video Downloader (479552792121059)
RECOMMENDATION:	Advanced Tech Review

KEY POINTS

- **Summary App Description:** The Facebook app Social Video Downloader ("SVM app") is purportedly an application to download videos from Facebook, and is related to two mobile applications: Video Downloader for Facebook, an Android application, and Social Video Player for Facebook, an iOS application.[1] These apps were created by a developer in India named Sandeep Nasa, who appears to be a solo developer and is responsible for a number of apps on the Facebook platform.
- **Reason for Secondary Review:** ALT
- **Summary of Findings:**

While conducting a background investigation of the SVM app and associated developer, the ADI Team discovered the app was conducting a phishing attack in which the app Redacted Redacted Redacted As the GAE app is developed by Facebook, and due to its use as an app for developers to test the Graph API, it has been approved through Facebook Login Review for all permissions. By having users log in through Redacted was potentially able to receive a Redacted

[1] See https://play.google.com/store/apps/details?id=com.xcs.fbvideos for the Android app and https://itunes.apple.com/in/app/social-video-player-for-facebook/id801877981?mt=8 for the iOS app.

Redacted

1. The SVM mobile app was Redacted Redacted
2. Through this technique, the Redacted Redacted
3. Detecting this type of attack is difficult for Facebook, as Redacted Redacted
4. Users of the SVM app would have had a defined expectation of privacy in that they granted the app certain permissions. By potentially circumventing those permissions, the app would have committed a serious violation of privacy and Facebook Platform Policies.

In order to dig further into the technical behavior of the SVM app, the ADI reviewed installs and API requests over time, as well the permissions profile across versions of the Graph API. After reviewing the installs over time of the original SVM app, as well as another Facebook app from the same developer titled SVM ("Second SVM app"), the ADI team observed a clear anomaly in which the number of installs for both SVM apps, as well as the GAE app, was several standard deviations above average on October 14, 2016. No evidence of explanatory external factors that could have caused this synced spike in installs has been found, and thus it raises the question as to whether the phishing attack began near this date.

Before this anomalous installation event, the number of installs and API requests per day for both SVM apps decreased at least linearly and continued to decrease after thereafter. This activity is concerning because if the app was in fact using GAE user tokens to make requests to the Graph API those requests were unauthorized and improperly attributed to the GAE app, both clear violations of Facebook Platform Policies. In order to determine whether this app was stealing user credentials, leveraging GAE access tokens, or violating policy in some other fashion the ADI team recommends an immediate Advanced Tech App Review and potential further action pending completion of the analysis.

---

[2] To be clear, this attack is not exploiting a flaw in the Graph API security model, but rather a flaw of human nature. Phishing attacks are designed to trick users into giving a program unauthorized access to data, and so because the user is the point of failure, they are very difficult to mitigate.

APP OVERVIEW

Identification of Related Apps

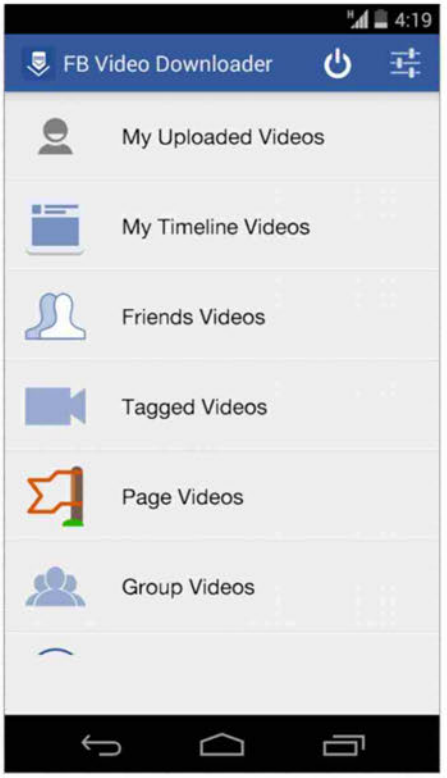
This report is specifically tailored to the SVM app; however, the following apps were also identified as associated with the same developer:

App ID	App Name	Total Authenticated Users	Earliest API Version Access	Relation to SVM App Developer
479552792121059	Social Video Downloader	9923149	1	√
1438510423132237	SVM	9213605	2.3	√
410861728958053	Quotes	2439	1	√
279163915588728	VidVee	1076	2	√
756557084369207	PhotoDownloader	514	1	√
641303925881006	Sketch FX	363	1	√
460731077291258	Quotes	118	1	√
106825679338453	Submit 2 Search Engine	5	1	√
855312924540146	Music To Videos	4	2.3	√
769890773051395	Photo Collage	4	2	√
545380148902343	Social Video Manager	2	1	√
382116955293423	Video Slides - Test1	2	2.2	√
352265314969934	Social Video Manager	1	2.2	√
577879492409081	Pic Lock	1	2.8	√
104220066279649	Submit 2 Search Engine	1	1	√
104377862930191	Submit 2 Search Engine	1	1	√
191327127627784	Android Goodies	1	1	√
751234254997989	Social Video Manager	1	2.3	√
769891143051358	Video Slides - Test1	0		√

By querying Hive, Facebook's internal data warehousing system, for apps related to the SVM app the ADI Team found 18 other apps created by the same developer. Approximately one-third of these apps had a total user count over 100, and only four had over 1,000 users. The two most popular apps were the SVM app and an app registered to Facebook as SVM ("Second SVM app"), which appears to be an abbreviation of "Social Video Downloader". Since this app is similar in name and user count to the SVM app, the rest of the analysis will focus on these two Facebook apps.

Understood Use Case of the App

The mobile apps associated with the Facebook SVM app were designed to allow users to download videos from Facebook, post them to a gallery that users of the app have access to, and share them with their friends. According to the Google Play Store, users could download videos "uploaded by you [users], videos you are tagged in, videos uploaded by your friends, videos from liked pages and groups too."[3] A screenshot captured from the Google Play Store is shown below:



[3] See https://web.archive.org/web/20140708223413/https://play.google.com/store/apps/details?id=com.xcs.fbvideos for the earliest link found to the app on the Google Play Store.

Reason for Escalation

Freeform Category	Freeform Response
Enforcement enforcement_freeform	Failed app privacy policy check in February 2014, March 2014, February 2018, and twice in March 2018.
Review History history_reviewed_freetext	Approved for user_videos which seems appropriate. Applied for user_likes with no good explanation; it was rejected correctly. Screenshot from app shows that you can also download friend's videos, which doesn't make sense with the permissions granted (users will only be able to download their own videos and videos they have been tagged in).
Mobile Review mobile_reviewable_freetext	Was able to download from Google Play store; app has been renamed "Video Downloader for Facebook". When signing into the app with Facebook, it prompts the user for "your public profile, friend list, timeline posts, videos, likes and email addresses" so somehow they are still getting user_likes, user_friends, and user_posts even though they don't have those permissions. Was able to download videos as promised. Seems really sketchy since the app is having you sign in through the Graph API Explorer (1st party app) which gives Social Video Downloader access to much more data than they'd normally be able to access, and would be more difficult to trace because the API requests aren't coming through this app ID.
Web Review web_reviewable_freetext	N/A

Other Freeform other_freeform	Privacy URL leads to a sketchy "Adobe Flash Player" download page. Couldn't find any further information on XCS Technologies from Google.
Final Response final_freeform	We should definitely investigate this app further and lock down Graph API Explorer if others are using this workaround to get access to user data.

APP ACTIVITY ANALYSIS

App Installation History

Users with the application currently installed: 9,923,149 users

Users who ever installed the app: 11,200,731 users

Install activity over time:

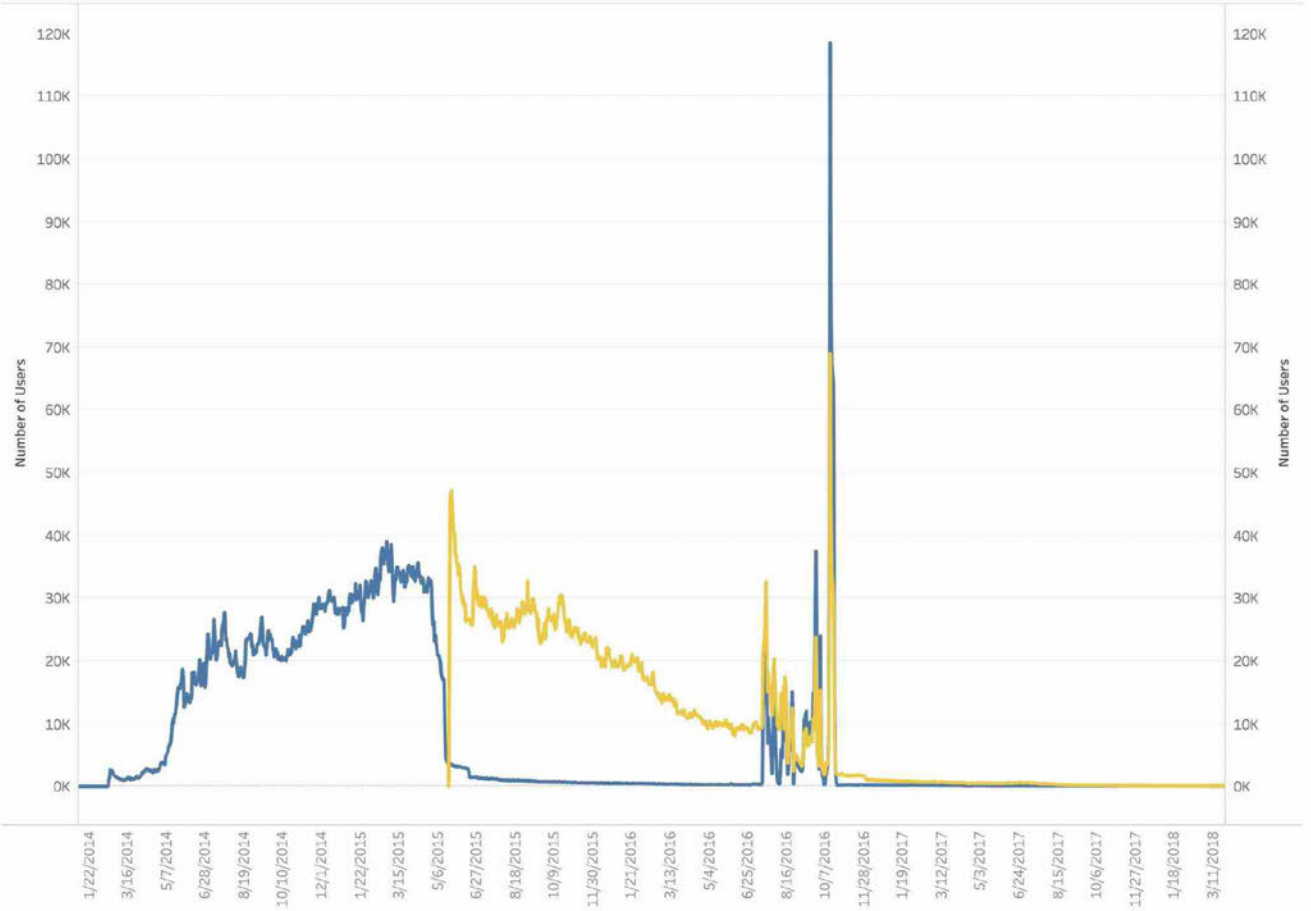


Figure 1. Installs by Day for SVM (Blue) and Second SVM (Yellow) Apps.

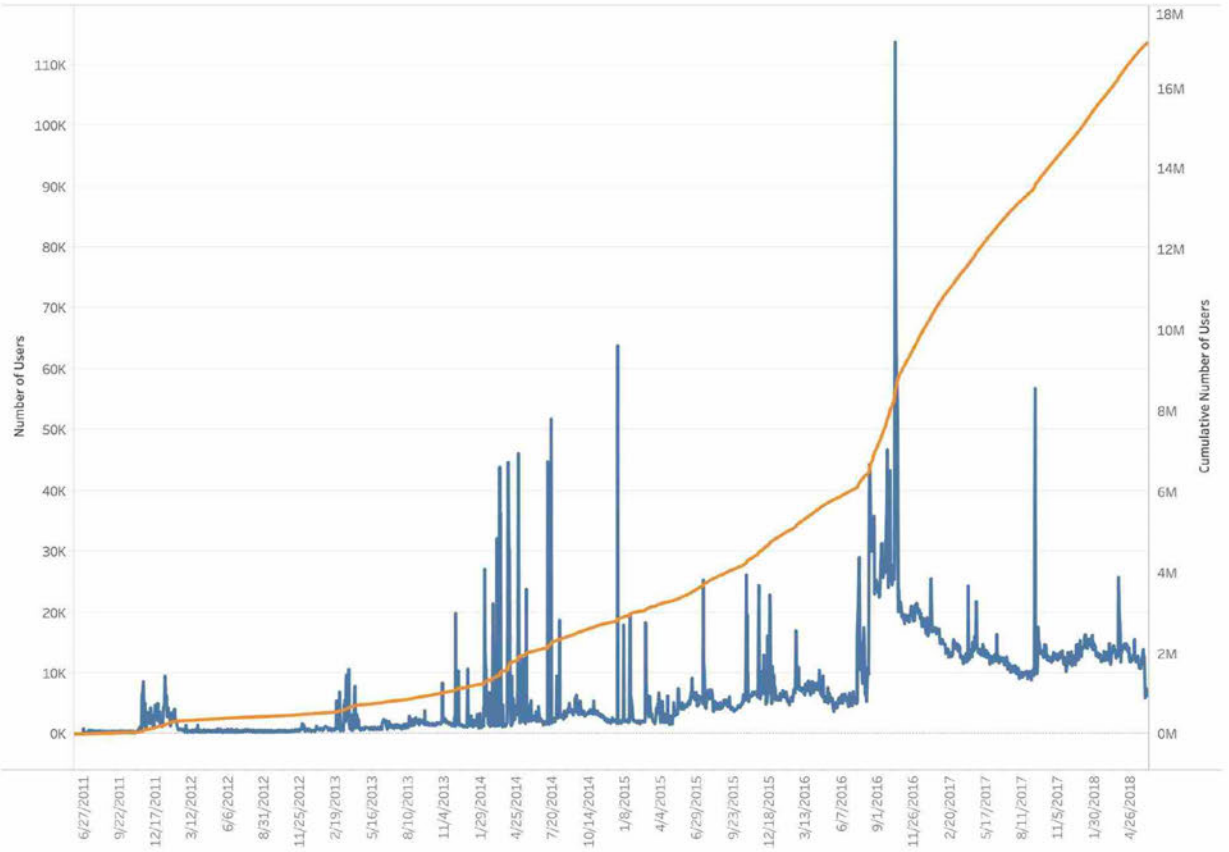


Figure 2. Installs by Day (Blue) for GAE App with Cumulative Number of Installs (Orange).

The graphs above show the installs by day for both the SVM and Second SVM apps, as well as the GAE app, and are illustrative of possible connections between all three. The SVM app was registered in July of 2013 and experienced a steady incline in installed users by day until April 28, 2015, approximately two days before version 1 of the Graph API was deprecated. The Second SVM app was registered on May 21, 2015, and installs for that app quickly eclipsed that of the SVM app, seeming to indicate the developer potentially intended to migrate users to this Facebook app. Given the similar names, apparent handoff in installs, and similar user counts, these two apps were likely utilized by the same mobile applications.

Beginning around July and leading into October of 2016, however, both the SVM and Second SVM apps experienced an anomalous spike in installs by day, with a particularly large installation event on October 14, 2016. Combined user installs for both apps on that day was 186,589, over 800% of the average daily installs before July of that year. Interestingly, the GAE app experienced a similarly large installation event on the same day, with a total of 113,736 installs. The ADI Team has not found any evidence of external factors to date to explain this coincidental spike in installs, and thus this raises an extremely concerning situation.

Assuming these observed anomalous installation events for all three apps were related, one of two situations was likely taking place:

1. Users would log in to the [redacted] This would mean users would be asked to enter their credentials twice.
2. Users would log in to the [redacted] and then [redacted] This would mean users would only be asked to enter credentials once, and the app was stealing user credentials.

Both scenarios described above are clearly against policy and should be grounds for being banned from the platform, but the second poses a greater threat to user security and privacy.

App Request and Permission History

Graph API v1.0

Summary

During version 1 of the Graph API, the SVM app had access to a concerning amount of sensitive user data, most of which does not seem necessary to the function of the app. In addition to friends likes, photos, videos, and profile information, the app had the user_manage_groups permission, which would have allowed it to pull information from any group a user was an admin of. With a total user base of 9,230,213 (before May 1, 2015), the potential affected population and the amount of sensitive data at risk are both very high.

Permissions

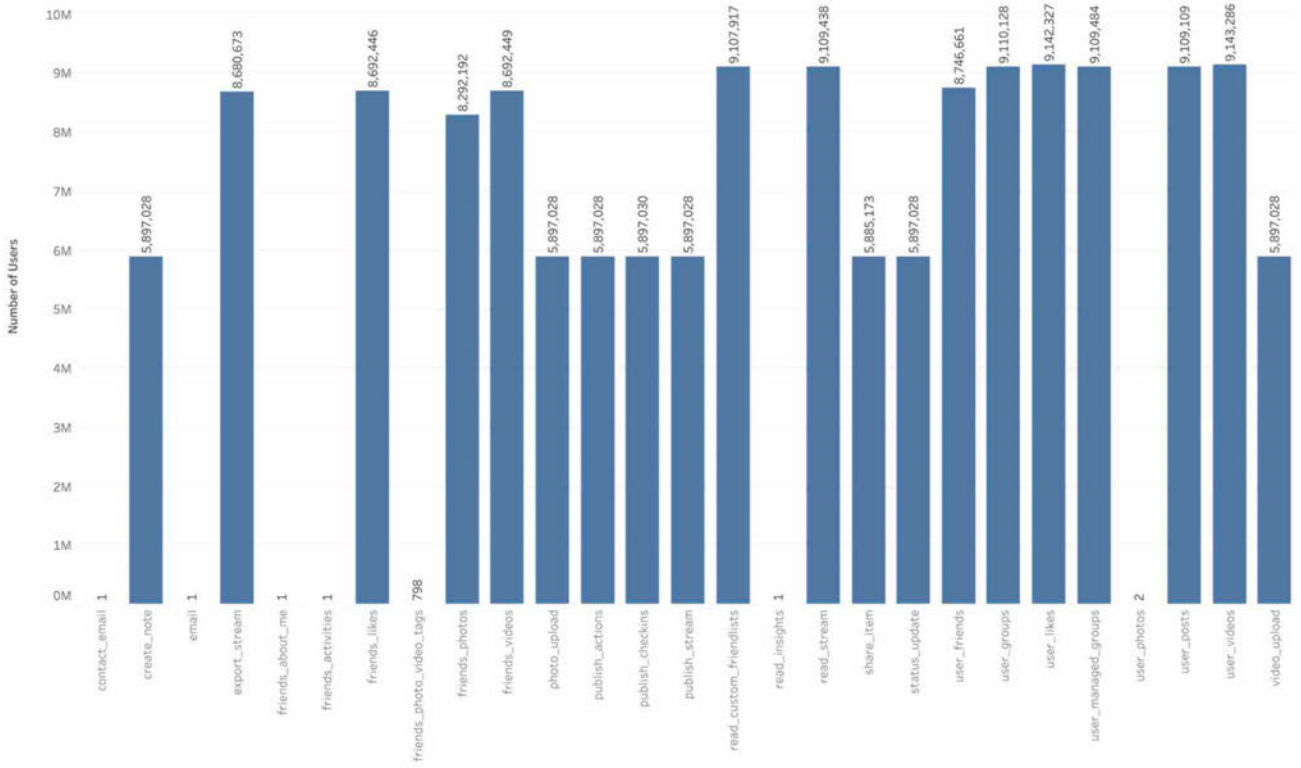


Figure 3. SVM App: Number of Users by Permission Granted (API Version 1.0)

Figure 3 above shows the expansive set of sensitive user data the SVM app had access to in version 1 of the graph API, such as user posts and activity feed (user_*, read_stream, export_stream), user friends' likes, photos, videos, and profile information (friends_*), as well as posts, comments, and likes from any group the users were administrators of. Most of these data would have been necessary to operate an app where users simply download and share videos from Facebook with each other, and thus may speak to ulterior motive by the developer.

Graph API v2.0-v3.0

Summary

Once version 1 of the Graph API was deprecated and the SVM app had to go through Login Review for extended permissions, the app lost access to most of the aforementioned concerning permissions and was left with user_friends and user_videos. These permissions make sense in the context of the app and are not concerning. However, this decreased access to sensitive user data coincided with the suspicious install anomalies, and thus the apps behavior post-version 1.0 warrants further review.

Permissions

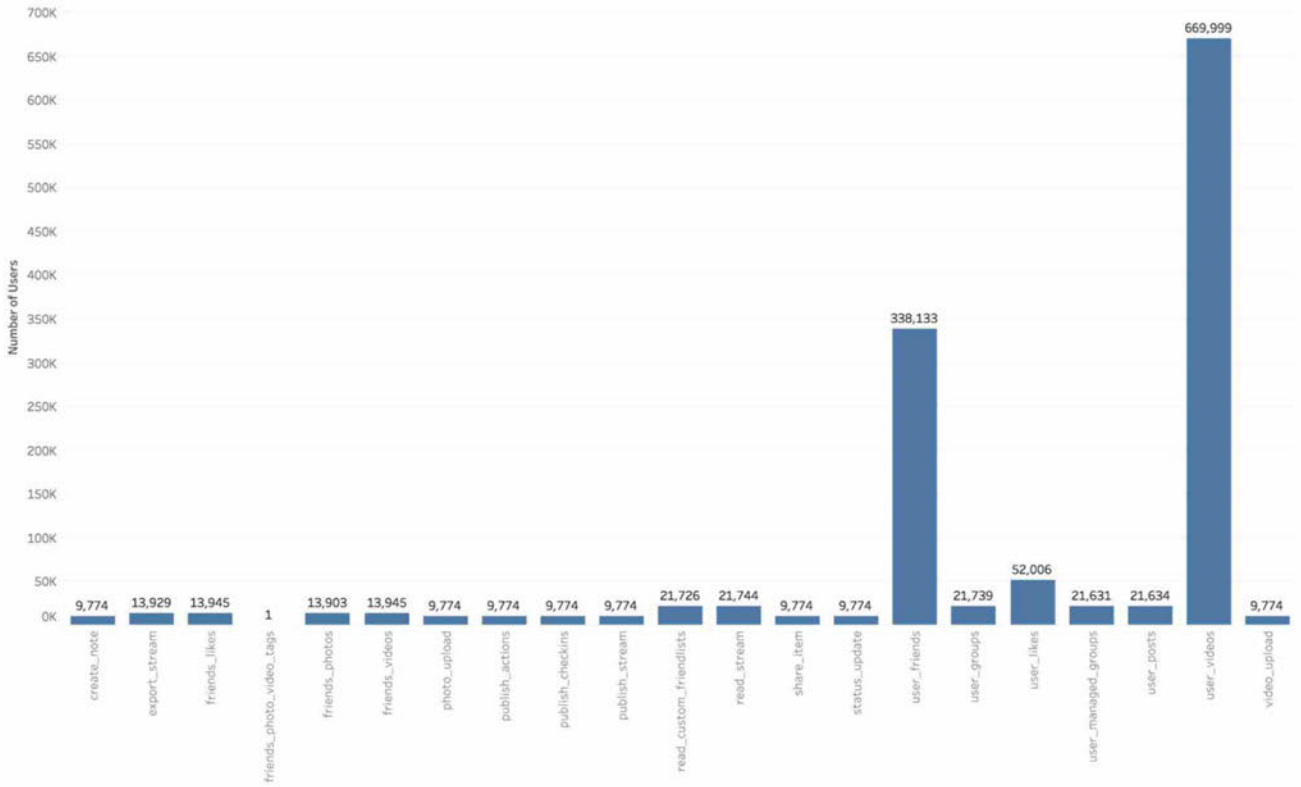


Figure 4. Number of Users by Permissions Granted (API Version >= 2.0)

After version 2.0 of the Graph API was released, the permissions granted to the SVM app were reduced significantly and scoped to those necessary to operating the app. The permissions profile for the Second SVM app mirrored those shown above, as that app was created after version 1 was deprecated. While the utlimate motive of the app developer cannot be derived from these data, in the scenario a malicious developer wanted to continue gathering sensitive user data without having to worry about Login Review, using the token for an app with more permissions would be one way to achieve that goal. This explanation could account for the drop in API requests and installs for the SVM and Second SVM app approximately a year after version 1 was deprecated, and could also potentially account for the mass installation event on October 14, 2016.

Graph API Changelog Archive

Version	Date Introduced	Date Deprecated
v1.0	4/21/2010	4/30/2014
v2.0	4/30/2014	8/7/2014
v2.1	8/7/2014	10/30/2014
v2.2	10/30/2014	3/25/2015
v2.3	3/25/2015	7/8/2015
v2.4	7/8/2015	10/7/2015
v2.5	10/7/2015	4/12/2016
v2.6	4/12/2016	6/13/2016
v2.7	6/13/2016	10/5/2016
v2.8	10/5/2016	4/18/2017
v2.9	4/18/2017	7/18/2017
v2.10	7/18/2017	11/7/2017
v2.11	11/7/2017	1/30/2018
v2.12	1/30/2018	5/1/2018
v3.0	5/1/2018	5/30/2018

Note: The ADI Team was not able to identify an archive for Quarter 1 of 2011; however, permission data was extracted for v1.0.